REMARKS

Claims 1-16 are pending. By this response, claim 13 is amended. Reconsideration and allowance based on the above amendments and following remarks are respectfully requested.

The Office Action objects to claim 13 suggesting amendment to the preamble. In response, Applicants have amended the claim in this manner. Applicants note that this amendment is non-substantive and is not being made in view of any of the cited prior art. Accordingly, withdrawal of the objection is respectfully requested.

Prior Art Rejection

The Office Action rejects claims 1-16 under 35 U.S.C. §103(a) as being unpatentable over Shaymov et al. (US 2002/0023227) in view of Osborne et al. (US 6,687,833). This rejection is respectfully traversed.

Each of independent claims 1, 9 and 13 refer to the preparation of a response to an illegal access by a communication device by a decoy server or data center located remotely from the network which received the illegal access. For example, claim 1 recites, *inter alia*, a decoy server, functionally coupled to the control system, wherein the apparatus is placed outside a given internal communication network, for receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network, and for taking countermeasures against the illegal access data received, further wherein the countermeasures include providing a response pretending to originate from the internal communication network, the response being encapsulated and sent to a network device within the given internal communication network to be decapsulated and transmitted by the network device to the data communication device. Claims 9 and 13 recite similar features.

In the embodiments of claims 1, 9 and 13, the entire response to the illegal access is developed by the decoy server or data center and also encapsulated by the decoy server or data center. This encapsulated response is then sent to the internal network where it is decapsulated and sent to the server from which the hacker originated.

In contrast, Shaymov teaches a system in which an intrusion detection system 110 sends intrusion information to a monitoring system by way of an analysis system 120 and network 10. The analysis system creates the response includes the decoyer origin information in the response and then sends this response back to the hacker. See Paragraphs 46 and 47. Thus, in Sheymov, the device (analysis system) that creates the response also sends this response back to the hacker. Therefore, encapsulation is unnecessary in the manner claimed by Applicants.

The Examiner states: "a monitoring center covertly (i.e., pretending) sends information to the analysis system removing the origin information of the monitoring center and the analysis center and in turn forwards the information to the hacker that includes the origin information of the original target ([0036]). The hacker would see the information as if it has been truly sent from the intended target." Applicants understand that Sheymov provides a decoy response to a hacker. However, the ultimate result is not what Applicants are claiming as the novelty. The process of obtaining a response and sending it to a hacker encompasses the novelty of the present invention. In this regard, the process steps of Sheymov particularly the monitoring center do not correspond to Applicants decoy server or data center. Specifically, the decoy center and data center as claimed by Applicants create the entirety of the response but do not send this response to the hacker. Instead, the response is encapsulated and sent back to the internal network for decapsulation and sending to the hacker. The use of a decoy server separate from the internal network, allows for multiple networks to use the decoy server and for better preparation of the response to the hackers. Sheymov does not teach this concept.

Further, Osborne does not remedy the deficiencies in Sheymov. It is agreed that Sheymov does not teach encapsulation for which Osborne is provided. Applicants respectfully submit, however, Sheymov is quiet about encapsulation because Sheymov's design does not require such it does lend itself for the need to perform encapsulation. Although Osborne teaches the concept of encapsulation, which Applicants have previously stated by itself is not novel, Osborne does not teach or suggest using encapsulation in a manner claimed by Applicants nor is this taught or suggest by Sheymov.

The Examiner states that because Osborne teaches about encapsulation all the limitations of the claims are met by Sheymov and Osborne. Applicants respectfully disagree. Osborne teaches a frame of data including data segments which are recursively encapsulated. These data segments correspond to protocol layers in a network and are part of the request frame receipt from the hacker. The object of Osborne is to represent accurately the response by also performing encapsulation within the response. See Col. 4, line 66 – Col. 5, line 26 (receipt of unauthorized frame) and Col. 7, lines 31-50 (creation of response using encapsulated data segments within). Thus, Osborne's response actually includes encapsulated segments in order to better represent the received data. This is the entire concept behind Oborne's teachings. The entire response itself is never encapsulated.

In terms of the presently claimed invention, Osborne's use of encapsulation amounts to nothing more than a general teaching of encapsulation. A decoy server is not taught by Osborne and certainly decapsulation of the response prior to sending to the hackers is not taught by Osborne. In fact, Osborne's response includes the encapsulation within the response. The entire response itself is never encapsulated as claimed by Applicants.

Osborne's general teaching of encapsulation does not lend itself to the specific application as claimed by Applicants. Further, the mere fact that a reference teaches a specific concept does not mean that it teaches each specific application of that concept. The question to be asked is would one of ordinary skill look to Osborne's teaching and Sheymov's teaching and be motivated to use each of these teachings to achieve Applicants claimed features. Applicants contend they would not. Sheymov's system is specific in that the analysis system performs the application of the decoy information in the response sent to a hacker. The analysis system also sends the response to the hacker. Thus, the analysis systems performs the development of the response, adding of decoy origin information and sending this to the hacker. Therefore, there is no need for encapsulation as in the presently claimed invention because the analysis system is directly sends the response which the analysis system created.

In embodiments of the present invention, the entire response to be sent to a hacker is developed by a decoy server or data center. This response must be sent to the internal network prior to sending to the hacker. Thus, encapsulation of the entire response is necessary otherwise the internal devices would not know the response is actually being sent from the decoy server or data server. It is within the internal network that the response is decapsulated and the sent to the hacker.

Neither Sheymov nor Osborne teach a separate decoy server or data center creating a response to a hacker where the entire response is encapsulated and sent back to an internal network for decapsulation of the entirety of the response and sending the response to the hacker. Simply stated, Sheymov teaches an analysis center that performs the creation of a response and also the sending of that response and thus encapsulation is not necessary. Osborne, at best, teaches receiving a frame which includes recursively encapsulated data segments and thus the creation of a response which also includes recursively encapsulated data segments in order for it to look more authentic. In Osborne, the entire response is never encapsulated and sent to an internal network. In Osborne, the created response with the data segments that are encapsulated therein is sent to the hacker.

Thus, Sheymov and Osborne fail to teach each and every feature of the independent claims. Further, one of ordinary skill in the art would not look to combine these teachings to achieve Applicants invention. Specifically in light of the fact that one would not look to encapsulate the created response in Sheymov if there is no need or motivation to do so since the analysis center also sends a response back to the hacker.

Therefore, Sheymov alone or in combination with Osborne fail to teach or suggest, *inter alia,* a decoy server functionally coupled to the control system, wherein the apparatus is placed outside an internal communication network, for receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network, therefore taking countermeasures against the illegal access data received, furthermore the countermeasures include providing a response returning to originate from the internal communication network, the response being encapsulated and sent to a network device within the given internal communication network to be decapsulated and transmitted by the network device to the data communication device, as recited in claim 1.

Sheymov and Osborne fail to teach, *inter alia,* taking internal measures against the illegal access data received by a data center remotely located from the internet from the internal network, and the countermeasures include providing a response pretending to originate from the internal communication network, response being encapsulated by the data center and sent to a network device within the internal communication network to be decapsulated and transmitted by the network device to the communication device, as recited in claim 9.

Also, Sheymov and Osborne fail to teach, *inter alia,* receiving an encapsulated unauthorized access packet at a data center placed outside the internal network ... analyzing the received packet to form a response packet; encapsulating the response packet so that it appears to originate from a target server; sending the encapsulating response packet to a network device, wherein the network device is within the internal network and wherein the network device decapsulates the encapsulated response packet and forwards the decapsulated packet to the source of the unauthorized access packet, as recited in claim 13.

In view of the above, Applicants respectfully submit that the combination of Sheymov and Osborne fail to satisfy the requirements under 35 U.S.C. §103 with regard to independent claims 1, 9 and 13. Further, dependent claims are also distinguishable from the cited references for the above reasons as well as for the additional features they recite. Accordingly, reconsideration and withdrawal of the rejections are respectfully requested.

Conclusion

For at least the above reasons, it is respectfully submitted that claims 1-16 are distinguishable over the cited art. Favorable consideration and prompt allowance are earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Chad J. Billings Reg. No. 48,917 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.14; particularly, extension of time fees.

Dated: September 12, 2007

Respectfully submitted,

By
Chad J. Billings
Registration No.: 48,917
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road, Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant